

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Policies and Rules
Concerning Toll Fraud

)
)
)
)

CC Docket No. 93-292

COMMENTS OF
YANGUARD CELLULAR SYSTEMS, INC.

Raymond G. Bender, Jr.
J.G. Harrington

Its Attorneys

DOW, LOHNES & ALBERTSON
1255 Twenty-third St., N.W.
Suite 500
Washington, D.C. 20037
(202) 857-2500

January 14, 1994

No. of Copies rec'd
List ABCDE

019

SUMMARY

The Commission's *Notice* on toll fraud is a valuable step in the effort to combat telecommunications fraud, and Commission attention to this issue is vital in light of the burgeoning growth of all forms of telecommunications fraud, including cellular fraud. Vanguard Cellular Systems, Inc. urges the Commission to take specific steps to give carriers and others the tools to fight fraud, to encourage every party affected by telecommunications fraud to work actively to prevent it and to make it possible to punish those who commit fraud.

First, the Commission should create its proposed anti-fraud council. Vanguard's experience in the cellular industry shows that cooperative anti-fraud efforts can bear fruit, and a broad-based anti-fraud council could draw expertise from all segments of the telecommunications industry. Facilitating cooperation between industry segments through an anti-fraud council could permit carriers, manufacturers and customers to find new solutions to the evolving problem of telecommunications fraud.

Second, the Commission can encourage the telecommunications industry to prevent and deter fraud by adopting the principle that the costs of fraud should be allocated based on whether the parties had taken reasonable steps to prevent fraud from occurring. This approach will create proper financial incentives for all parties potentially affected by fraud. The anti-fraud council can help the Commission determine what anti-fraud measures are appropriate for each industry segment.

Finally, the Commission should take steps to punish the perpetrators of fraud. The Commission should promptly adopt its proposed rule prohibiting manufacture of cellular phones with alterable electronic serial numbers, and should enforce the rule vigorously. The Commission also should recommend and encourage legislative action to target telecommunications fraud and the manufacture of equipment used to commit telecommunications fraud, at both the federal and state levels.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. AN ANTI-FRAUD COUNCIL WILL HELP THE TELECOMMUNICATIONS INDUSTRY COMBAT FRAUD EFFECTIVELY.	3
III. ALLOCATION OF LIABILITY BASED ON THE ABILITY TO PREVENT FRAUD WILL ENCOURAGE CARRIERS AND OTHER PARTIES TO TAKE STEPS NECESSARY TO MINIMIZE THE COSTS OF FRAUD	5
IV. STRINGENT PENALTIES FOR PARTIES THAT PERPETRATE FRAUD ARE A NECESSARY ELEMENT OF ANY COMMISSION PROGRAM TO REDUCE FRAUDULENT USE OF THE NATION'S TELECOMMUNICATIONS SYSTEMS . . .	8
A. The Commission Should Adopt and Enforce Rules that Prohibit Manufacturing or Altering Cellular Telephones in Ways that Facilitate Fraud	8
B. The Commission Should Recommend Legislative Action to Deter Fraud	10
V. CONCLUSION	11

RECEIVED

JAN 14 1994

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

Policies and Rules
Concerning Toll Fraud

)
) CC Docket No. 93-292
)
)

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

COMMENTS OF VANGUARD CELLULAR SYSTEMS, INC.

Vanguard Cellular Systems, Inc. ("Vanguard"), by its attorneys, hereby submits its comments in the above-referenced proceeding.^{1/} This proceeding marks an important step in the Commission's efforts to combat fraud and its effects on carriers and customers alike. Vanguard believes the Commission should establish policies to encourage carriers to adopt measures that will minimize the opportunity for telecommunications fraud to occur. Such measures should include creating an anti-fraud council and adopting rules that give carriers an incentive to detect and prevent fraud. It is vital for the Commission to assure that anti-fraud efforts are coordinated among all carriers, not fragmented along increasingly artificial industry lines.

I. INTRODUCTION

Vanguard began providing cellular service in 1985 and is today the second largest operator of purely non-wireline cellular systems in the United States. The company owns and operates cellular systems serving 18 MSAs and four RSAs and holds minority interests in more than 50 other cellular systems. Vanguard's cellular systems covers a geographic area containing more than 6.2 million people and provide

^{1/} Policies and Rules Concerning Toll Fraud, *Notice of Proposed Rulemaking*, CC Docket No. 93-292 (rel. Dec. 2, 1993) (the "Notice").

service to more than 135,000 subscribers utilizing approximately 110 cell sites. In 1993, Vanguard's revenues exceeded \$110 million, a 35 percent increase over 1992 revenues.

Like most cellular carriers, Vanguard has had to confront fraud, both in its service area and by perpetrators operating in other markets but using telephone numbers that are assigned to Vanguard. Fraud is a large and growing problem for all cellular carriers in the industry. While fraud has been concentrated in large cities, cellular roaming fraud affects all carriers and fraud in smaller markets is growing as well. Moreover, as cellular technology evolves, techniques for perpetrating fraud also evolve, forcing carriers to develop ongoing responses. As a consequence of its concerns about fraud, Vanguard has been an active participant in the Cellular Telephone Industry Association's ("CTIA") ongoing fraud task force. Experience gained from that participation has demonstrated for Vanguard the value of coordinating industry efforts to combat fraud.

Because coordinated efforts are vital to detecting and preventing fraud, the Commission's focus should be on adopting rules that encourage carriers to cooperate to prevent fraud. The first element of the Commission's program should be to facilitate cooperation through an anti-fraud council, as suggested in the *Notice*. The anti-fraud council should permit participation by all carriers and end users, and serve as a clearinghouse for information about how fraud is committed and how it can be prevented. Second, the Commission should adopt liability rules for fraudulent calls that allocate the costs of fraud based on the ability of each affected party to prevent it.

Finally, the Commission should adopt and vigorously enforce rules that penalize parties that perpetrate fraud; and it should encourage federal and state legislative authorities to pass and enforce criminal sanctions for the commission of telecommunications fraud.

II. AN ANTI-FRAUD COUNCIL WILL HELP THE TELECOMMUNICATIONS INDUSTRY COMBAT FRAUD EFFECTIVELY.

The *Notice* seeks comment on whether the Commission should establish a new Federal Advisory Committee on telecommunications fraud issues. *Notice* at ¶ 13. Vanguard wholeheartedly endorses this proposal.

An advisory committee could serve several purposes. First, it can help the Commission to understand how fraud is occurring and what steps are available to consumers, the manufacturing industry, service providers and the Commission to help combat it. By acting as a clearinghouse, an advisory committee can facilitate the swift dissemination of critical information in time to design solutions to address new types of fraud before they become serious problems.

An advisory committee also can facilitate cooperation among carriers, and between carriers and equipment manufacturers. As the *Notice* makes clear, fraud is not just a CPE problem, an interexchange carrier problem or a cellular carrier problem. In many cases, the only effective approaches to combat fraud require different parties to work together. For instance, in the cellular industry, roamer validation is an important element in preventing some kinds of fraud, but is possible only if the home carrier and the carrier providing service form a cooperative

relationship to work together. Other fraud detection and prevention techniques, such as pre-call validation using Signalling System 7, also require carriers to cooperate, by passing data across their networks to validate calls or in other ways.

Vanguard's experience with CTIA's fraud task force reinforces the value of industry cooperation to prevent fraud. By facilitating communication between cellular carriers, the CTIA task force has made it easier for carriers to identify fraudulent activities and focus on ways to prevent those activities. The CTIA task force also has fostered an environment in which cellular carriers are willing to alert each other to regional problems, even when two carriers are competing with each other. Vanguard had such an experience recently, and the willingness of a Vanguard competitor to provide information about the activities of a perpetrator of subscription fraud afforded Vanguard the opportunity to cut off the perpetrator's service before he had a chance to cause significant harm. Vanguard firmly believes that cellular industry cooperation has reduced the harm caused by fraud and that continued cooperation is necessary to detect and prevent fraud in the future.

The Commission's own experience with advisory committees also demonstrates how industry cooperation can further important public policy goals such as preventing fraud. The Network Reliability Council has been justly praised for its efforts to identify and address issues affecting the reliability of telephone networks. Most recently, the Advisory Committees established to assist the negotiated rulemakings for mobile satellite services were extremely helpful in furnishing technical advice and advising the Commission on practical industry concerns that needed to be addressed

by Commission rules and policies.^{2/} It is clear that advisory committees are particularly useful to the Commission in addressing highly complex, fast-developing technical matters, like the mobile satellite services and toll fraud.

For these reasons, Vanguard firmly supports the Commission's proposal to establish an advisory committee on telecommunications fraud and urges the Commission to fully involve all segments of the telecommunications industry in the advisory committee's processes. In light of the practical experience it has gained in the marketplace, as well as its involvement with the CTIA task force on cellular fraud, Vanguard would be willing to provide a representative to serve on a Commission advisory committee should the Commission so desire.

III. ALLOCATION OF LIABILITY BASED ON THE ABILITY TO PREVENT FRAUD WILL ENCOURAGE CARRIERS AND OTHER PARTIES TO TAKE STEPS NECESSARY TO MINIMIZE THE COSTS OF FRAUD.

One of the most significant and overriding questions raised by telecommunications fraud is who should bear the costs of that fraud. In one sense, all legitimate users of telecommunications services pay for fraud, but current policies also effectively allocate those costs to specific parties. The *Notice* asks if it would be appropriate to reallocate the costs of telecommunications fraud. *See Notice* at ¶ 25. Vanguard submits that the Commission should consider adopting allocation principles

^{2/} See Amendment of Section 2.106 of the Commission's Rules to Allocate the 1610-1626.5 MHz and the 2483.5-2500 MHz Bands for Use by the Mobile-Satellite Service, Including Non-geostationary Satellites, *Report and Order*, ET Docket No. 92-28, FCC 93-547 (rel. Jan. 12, 1994) at ¶¶ 9-10.

that impose the costs of telecommunications fraud on the party that is best able to prevent fraud and to avoid the costs it creates.

The *Notice* describes two divergent approaches to toll fraud in the *Chartways* and *United Artists* cases. *Notice* at ¶ 8-9. The results of these cases are consistent with a broader principle, however, which is that the party that can best prevent telecommunications fraud, but which refuses to take steps to do so, should bear the burden of it. Otherwise, it is possible, indeed likely, that the party that can prevent fraud actually will profit from it.

Cellular roaming fraud provides a good example of this principle. Under the standard roaming agreements in place across the country, a carrier is responsible for paying for all roamer calls made by cellular phones with numbers in the range assigned to that carrier, whether or not the calls are legitimate. The home carrier, despite its liability for all calls, has little ability to monitor or prevent fraudulent calls that take place on another carrier's system.^{3/} The carrier providing service does have the ability to detect and prevent fraudulent calls, for instance through software that detects the patterns of ESNs transmitted by cellular phones altered to have tumbling ESNs, but it has little incentive to do so because the serving carrier is entitled to full payment even for fraudulent calls.

3/ A home carrier can make a database listing of all active numbers and their associated electronic serial numbers ("ESNs") available for use in validation of calls, and almost every carrier does so. The carrier providing the service uses this database to validate calls after they have started. This prevents repeated use of a phone with an invalid telephone number or ESN. As the *Notice* recognizes, however, this approach cannot prevent fraudulent calls from telephones with so-called "tumbling" ESNs, which are a significant problem in the cellular industry. *Notice* at ¶ 33.

Vanguard has attempted to confront this problem by renegotiating roaming agreements to limit its liability for fraudulent calls to the serving carrier's direct costs, but this is only a partial solution to the problem. At best, Vanguard's agreements leave serving carriers indifferent to roaming fraud, rather than creating an active incentive to prevent it.

If the Commission adopted principles that allocated the costs of fraud based on whether a party had taken all reasonable steps to detect and prevent fraud, then all carriers would have appropriate financial incentives to cooperate in addressing this problem. Any measure that would be cost effective would be adopted, at least by any carrier that wanted to limit its liability for fraud.^{4/} In the cellular context, serving carriers in high fraud areas would have an incentive, for instance, to install the software necessary to detect tumbling ESNs. Carriers in low risk areas, such as rural cellular licensees, also will not be forced to adopt anti-fraud measures that are not cost effective for their markets. Allocating the costs of fraud in this way also will avoid saddling carriers with relatively little ability to prevent fraud on their own, such as long distance resellers, with costs that should be borne by parties with the power to attack fraud. While it may take some time to determine appropriate allocations, it

4/ This allocation principle also would be economically efficient because it will not require carriers to adopt any particular measures to prevent fraud but would give them an incentive to do so if doing so were justified in a particular case. For instance, if a carrier determines that its likely liability for a particular kind of fraud is \$100,000, but the preventive measure costs \$200,000, a carrier might choose to bear the cost of any fraud that occurs rather than spend an excessive amount to cure the problem. Turning the situation around, a carrier that could expect to prevent \$200,000 in fraud with an expenditure of \$100,000 almost certainly would choose to adopt the preventive measure.

will be worth the effort. Long term progress against telecommunications fraud is likely only if all affected parties have real incentives to detect and prevent it.

An advisory committee also can play an important role in this area. The committee could help to determine what steps carriers, manufacturers and users should reasonably take to prevent fraudulent activities. The Commission then could use that information to determine how the costs of fraud should be allocated.

IV. STRINGENT PENALTIES FOR PARTIES THAT PERPETRATE FRAUD ARE A NECESSARY ELEMENT OF ANY COMMISSION PROGRAM TO REDUCE FRAUDULENT USE OF THE NATION'S TELECOMMUNICATIONS SYSTEMS.

The efforts of carriers, equipment manufacturers and customers to prevent telecommunications fraud are only half of the fraud prevention equation. Without significant penalties for perpetrators, the success of the battle against fraud will be greatly limited. This is particularly true in the cellular industry, where most fraud is made possible by the illicit alteration of cellular telephones. The Commission should adopt and vigorously enforce rules against such alterations and should recommend specific legislation to outlaw equipment-based cellular fraud.

A. The Commission Should Adopt and Enforce Rules that Prohibit Manufacturing or Altering Cellular Telephones in Ways that Facilitate Fraud.

As described above and in the *Notice*, most cellular fraud results from the use of cellular telephones that have been manufactured or altered to facilitate fraud. Tumbling ESNs and "cloned" cellular phones, as the *Notice* reports, are responsible for the bulk of the monetary losses from cellular fraud. *Notice* at ¶ 33. CTIA

estimates place the cost of cellular fraud at \$300 million in 1992, and it is estimated today to be in excess of \$1 million a day. This fraud would be impossible if the phones that are being used were operating in accordance with the manufacturing and design standards for cellular telephones. The Commission should adopt rules and vigorously enforce rules that specifically prohibit the alterations that make tumbling ESNs and cloning possible.

Commission guidelines already prohibit alteration of ESNs. See OST Bulletin No. 54, ¶ 2.3.2 (1983) (stating that ESNs must be unique, factory-set and not readily alterable in the field). The Commission also has determined that changing ESNs is a violation of Section 22.915 of the Commission's Rules. See Public Notice, "Changing Electronic Serial Numbers on Cellular Phones Is a Violation of the Commission's Rules," Rep. No. CL-92-3 (rel. Oct. 2, 1991). Nevertheless, most cellular fraud occurs as the result of operation of phones that have altered or alterable ESNs. There are even companies openly advertising that they will clone cellular phones. Thus, it is clear that more explicit rules and vigorous enforcement are necessary.

First, the Commission should act swiftly to adopt proposed Section 22.929 of the Commission's Rules. This proposal is part of the general Part 22 rewrite proceeding, which now has been pending for more than a year.^{5/} While the extensive modifications to the Commission's Rules that are contemplated in that

^{5/} Revision of Part 22 of the Commission's Rules Governing the Public Mobile Service, *Notice of Proposed Rulemaking*, 7 FCC Rcd 3658, 3741 (1992) (proposing new Section 22.929).

proceeding may well justify continued deliberation in some areas, there is no reason why the Commission cannot now adopt this one rule without deciding the entire rulemaking.^{6/} Prompt adoption of Section 22.929 will give the Commission an important tool in attacking the perpetrators of cellular fraud.

Second, the Commission must make a commitment to use its forfeiture authority to enforce its anti-fraud rules. Unenforced rules have little or no effect. On the other hand, if individuals or companies that make cellular phones with tumbling ESNs or that clone cellular phones know that the Commission will seek them out and impose substantial forfeitures, they will be much less inclined to engage in these illicit business activities.

B. The Commission Should Recommend Legislative Action to Deter Fraud.

The Commission's enforcement efforts will be important, but criminalization of telecommunications fraud is equally vital. The Commission should recommend to Congress that specific criminal laws covering telecommunications fraud and activities that facilitate telecommunications fraud be enacted.

Criminal laws are important because in many cases the Commission's forfeiture authority will not deter parties that perpetrate fraud. These parties may be effectively judgment proof, but they are not immune to incarceration and other

^{6/} The Commission has followed such a course in many other proceedings in the past. See, e.g., Policies and Rules Concerning Rates for Dominant Carriers, *Report and Order and Second Further Notice of Proposed Rulemaking*, 4 FCC Rcd 2873 (1989) (adopting price cap rules for AT&T, but deferring decision for local exchange carriers).

criminal penalties. Criminalizing telecommunications fraud, and especially cellular fraud, will give those who might perpetrate fraud a meaningful reason not to do so.

Such legislation has been introduced in a number of states across the country, but federal criminal legislation is important in its own right. While telecommunications fraud often is covered under general fraud and theft statutes, specific criminal penalties for telecommunications fraud will highlight the nature of the problem and give prosecutors a tool that is fitted to the crime. In this regard, and in addition to pressing for federal legislation, the FCC should encourage state legislatures and regulatory authorities to adopt and enforce stringent criminal and other measures to combat telecommunications fraud.

Moreover, current statutes do not cover possession or manufacture of equipment that is used for cellular fraud. As noted above, without telephones with tumbling ESNs or cloned telephones, most current cellular fraud would not be possible. Since these telephones are used almost exclusively for fraudulent purposes, there is no reason to permit their possession or manufacture. The Commission should therefore recommend that Congress and state legislatures prohibit possessing cellular telephones with tumbling ESNs or that are cloned, manufacturing phones with tumbling or alterable ESNs or altering existing phones to clone them or give them tumbling ESNs.

V. CONCLUSION

Telecommunications fraud is a serious and growing problem that should be addressed swiftly and continuously. The Commission can help to stem the growth of

fraud in several ways. It can create a fraud advisory committee as a forum for the telecommunications industry to foster cooperation and prompt responses to new forms of fraud. It can adopt allocation principles that encourage parties that can prevent fraud to do so. Finally, the Commission can take steps to prohibit and punish parties responsible for telecommunications fraud, particularly those responsible for equipment-based cellular fraud, and it can encourage federal and state legislative authorities and state regulators to adopt criminal and other sanctions for the commission of telecommunications fraud. For these reasons, Vanguard urges the Commission to act in accordance with the recommendations contained in these comments.

Respectfully submitted,

VANGUARD CELLULAR SYSTEMS, INC.

By: 

Raymond G. Bender, Jr.

J.G. Harrington

Its Attorneys

Dow, Lohnes & Albertson
1255 23rd Street, N.W., Suite 500
Washington, D.C. 20037
(202) 857-2500

January 14, 1994

CERTIFICATE OF SERVICE

I hereby certify that on this 14th day of January, 1994, copies of the foregoing "Comments of Vanguard Cellular Systems, Inc." were served by first class, United States mail, postage prepaid, upon the following parties, except where indicated:

*The Honorable Reed Hundt
Chairman
Federal Communications Commission
1919 M Street, N.W., Room 814
Washington, D.C. 20554

*The Honorable James Quello
Commissioner
Federal Communications Commission
1919 M Street, N.W., Room 802
Washington, D.C. 20554

*The Honorable Andrew Barrett
Commissioner
Federal Communications Commission
1919 M Street, N.W., Room 844
Washington, D.C. 20554

*The Honorable Ervin Duggan
Commissioner
Federal Communications Commission
1919 M Street, N.W., Room 832
Washington, D.C. 20554

*Kathleen Levitz
Acting Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W., Room 500
Washington, D.C. 20554

*John Cimko, Jr.
Chief, Mobile Services Division
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W., Room 644
Washington, D.C. 20554

***Myron Peck**
Deputy Chief, Mobile Services Division
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W., Room 644
Washington, D.C. 20554

A handwritten signature in cursive script, reading "Tammi A. Foxwell". The signature is written in dark ink and is positioned above a horizontal line.

Tammi A. Foxwell

***Via hand delivery.**